**Threat Modeling and Risk Management Use Cases (Cyber)**

**Table of Contents**

**DRAFT**

[1. Background 1](#_Toc387334115)

[2. Use Case Overview 2](#_Toc387334116)

[3. Use Cases 3](#_Toc387334117)

[3.1 Enhanced Shared Situational Awareness Use Cases 3](#_Toc387334118)

[3.1.1 Overview of Information Sharing Architecture 4](#_Toc387334119)

[3.1.2 Definition of ISA Functions 4](#_Toc387334120)

[3.1.3 ISA Enduring Functional Exchanges (EFEs) and Subcomponents 5](#_Toc387334121)

[3.1.4 Configuration/ Anomaly Reporting 6](#_Toc387334122)

[3.1.5 Knowledge of Threat Actors 7](#_Toc387334123)

[3.1.6 Incident Awareness 7](#_Toc387334124)

[3.1.7 Indications & Warnings 8](#_Toc387334125)

[3.1.8 Vulnerability Knowledge 9](#_Toc387334126)

[3.1.9 Mitigation Strategies 10](#_Toc387334127)

[3.1.10 Mitigation Actions and Responses 10](#_Toc387334128)

[3.2 Victim Notifications 12](#_Toc387334129)

[3.2.1 Victim information compromised as part of a cyber-intrusion 12](#_Toc387334130)

[3.2.2 Victim is directly involved in a cyber-enabled crime 13](#_Toc387334131)

[3.3 Justice and Public Safety 14](#_Toc387334132)

[3.3.1 Cyber Intrusion Sharing 14](#_Toc387334133)

[3.3.2 Cyber Enabled crimes/ Investigatory Referrals 14](#_Toc387334134)

[3.3.3 Fusion Center Cross-Domain Sharing 15](#_Toc387334135)

[Appendix A—Document History 16](#_Toc387334136)

# Background

Multiple communities have developed data and exchange schema and interfaces for sharing information about threats, risks and incidents that impact important government, commercial and personal assets and privacy. While each of these schema and interfaces provides value for a specific community it is difficult to federate these multiple representations to arrive at broad-based situational awareness and enact the appropriate courses of action. Cyber related attacks have added a new dimension that stresses traditional mitigation strategies.

The Threat Modeling and Risk Management initiative calls for a conceptual model for threats and risks that unifies the semantics of and can provide a bridge across multiple threat and risk schema and interfaces. The conceptual model will be informed by and mapped to high-level elements in existing schema as defined by STIX (A Cyber information sharing specification) and existing NIEM domains. This will enable combined Cyber, physical, criminal and natural threats and risks to be federated, understood and responded to effectively.

The effort will initially focus on developing the broad threat model. This model will be further refined using mission specific use cases that provide the details of the business problem, the stakeholders/actors involved, business rules, detailed data elements and any policy elements associated with access control.

# Use Case Overview

The ‘Threat Model and Risk Management’ initiative focuses on 3 key aspects:

* Open Community based approach
* Cross Domain information sharing requirements
* Model Drive Approach

The following section describes the use cases relevant to this project. The use cases fall in the following 3 categories:

* “wishes cases”, not really use cases but high level descriptions of some need, these will then require a domain expert to work with to nail down the requirements.
* Requirements use cases, probably with some example that we could really use (e.g. the STIX example) and indication of the kind of data and level of detail.
* Baseline models/schemas from which we can factor/abstract into the conceptual model (e.g. SAR)

# Use Cases

This section includes descriptions for the mission use cases:

## Enhanced Shared Situational Awareness Use Cases

National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23) (Reference 4) helps to establish the US policy, strategy, guidelines, and implementation actions required to secure the United States in cyberspace to include military, Federal, and civilian assets. NSPD-54/HSPD-23 includes a Comprehensive National Cybersecurity Initiative (CNCI) that provides the impetus to execute a number of key initiatives. Of those, CNCI-5 (Connect the Centers to Enhance Cyber Situational Awareness) directed the development of a detailed plan, including standard operating and notification procedures that connect designated Cybersecurity Centers to enhance situational awareness of the overall Cyberspace Domain. The intent is to enable practical mission bridging across all US cyber elements by providing an enhanced real-time Shared Situational Awareness (SSA) capability, thus supporting Integrated Operational Action (IOA) mechanisms to improve the security of US Government assets and protect the critical infrastructure in which they depend. This definition of CNCI-5 was expanded to include interactions with foreign partners.

In 2010, a group composed of representatives from each CNCI-5 designated Cybersecurity Center was established to support planning, development, and implementation of an information sharing architecture that defines the functions, activities, and information exchanges within and among Cybersecurity Centers to support CNCI-5 objectives. The group inherited its authority from the participating organizations: US Cyber Command Joint Operations Center (JOC), Defense Cyber Crime Center (DC3), National Cyber Investigative Joint Task Force (NCIJTF), Intelligence Community Incident Response Center (IC-IRC), National Security Agency/Central Security Service (NSA/CSS) Threat Operations Center (NTOC), and National Cybersecurity and Communications Integration Center (NCCIC).

The ISA Framework emphasized developing a common vernacular and point of reference from which the Centers could begin to articulate operational and technical needs. The interagency group subsequently identified formal requirements that must be met to enable solutions to be specified and deployed.

This ISA SSA Requirements Document is an element of the ISA, defined by the following collection of products:

* + **ISA Framework** –This document provides the common vocabulary and understanding of functional elements and exchanges among the various Cybersecurity Center partners and stakeholders. It assists in the identification of technical and operational needs to support the implementation investment and development planning.
  + **ISA SSA Requirements Document** – This document translates the ISA framework to a 'buildable' architecture, defined as a set of enterprise requirements drivers and community standards that guide national investment in SSA and the addition of new partners.
  + **ISA Technical Implementation Plan** – This document provides a Technical Architecture Roadmap to implement the ISA starting at the end of FY13 extending through FY18 and coordinates implementation roadmaps from each ISA Participant.

The ISA Framework is not an end in and of itself. Each ISA Participant agrees on commonly provisioned standards and solutions and then implements, manages, and maintains the capabilities. An ***ISA Participant*** is defined as an organization that performs any of the ISA Functions defined in the ISA Framework and has accepted that information sharing, as defined by the ISA, is a part of the organization’s cybersecurity mission. Using the ISA SSA Requirements Document, ISA Participants can trace to their own capabilities, or derive performance requirements supportive of their own operations. Note that it is possible for an ISA Participant to pass their information through another ISA Participant, and therefore achieve the satisfaction of these requirements [e.g., Critical Infrastructure/Key Resources (CIKRs) organizations may leverage NCCIC capabilities].

This ISA SSA Requirements Document consists of three components: Mission, Information, and Technical requirements. The Mission component characterizes the activities that drive information sharing needs. The Information component defines what information is shared by whom and what that information looks like (i.e., delineating the data format to be used and defining the standard set of required data tags). The Technical component defines the capabilities required to achieve the envisioned national/collaborative cybersecurity SSA.

### Overview of Information Sharing Architecture

The ISA Framework (Reference 1) abstracts Participant’s operational roles into a comprehensive set of functions. It connects the functions and series of information exchanges to collectively describe the information needed to support the envisioned national SSA necessary to enable IOA. IOA is defined as a series of coordinated actions undertaken by those who have both the capability and authority to take the action.

Although the ISA functions may not represent every internal activity that an ISA Participant might perform, they are intended to capture and categorize all major activities that are associated with information sharing. These Participants can benefit from each other’s shared experiences - and should do so. However, each Participant has a unique mission to perform, their own data to analyze and actions to take. Each Participant must have the capability to continue to operate, even in the absence of the other Participants, to the best of their ability.

### Definition of ISA Functions

|  |  |
| --- | --- |
| **ISA Function** | **Definition** |
| Network Operations Function (NOF) | Cybersecurity activities that are performed by those managing a network |
| Computer Network Defense Function (CNDF) | Cybersecurity activities that are performed within a network to detect and mitigate anomalous behavior |
| Domain/Sector Awareness Function (DSAF) | Aggregation, synthesis, filtering, and release of information to other centers and partners to enhance their situational awareness while monitoring the health and performance of their own networks |
| Threat Assessment Function (TAF) | Discovery, characterization, and development of mitigation strategies to counter existing and emerging cybersecurity threats |
| Threat Operations Function (TOF) | Planning for*,* executing, and monitoring the effects of a cyber-action that takes place in the adversary's virtual or physical space |
| IOA Planning Function (IOAPF) | Planning Activities associated with developing an integrated action plan across multiple Participants to include: development of actions and comprehensive mitigation plans, considering assessments across multiple areas of risk, mission impact and achievable effects. |
| IOA Coordination Function (IOACF) | Coordinating activities associated with the execution of an integrated action plan, including initiating mitigation plans and exchanging information to coordinate interrelated activities during execution, monitoring progress of mitigations, and assessing the relative success of those mitigations. |

### ISA Enduring Functional Exchanges (EFEs) and Subcomponents

The information exchanges between the ISA Functions are defined in terms of the ISA EFEs. Within each EFE, there are a series of subcomponents that represent various data types.

|  |  |  |  |
| --- | --- | --- | --- |
| **EFE #** | **EFE Name** | **Subcomponent ID** | **Subcomponent Name** |
| **1** | Configuration / Anomaly Reporting | 1a | Risk Posture |
| 1b | Anomalies |
| 1c | Infrastructures |
| **2** | Knowledge of Threat Actors | 2a | Threat Actor Infrastructure |
| 2b | Threat Actor Personas |
| 2c | Threat Actor Attribution |
| 2d | Trend Analysis |
| 2e | Victim Information |
| 2f | Threat Actor Indicators |
| **3** | Incident Awareness | 3a | Incident Information |
| 3b | Computer Network Operations (CNO) Awareness |
| 3c | Incident Data |
| 3d | Infrastructure Impact/Effects |
| 3e | Victim Information |
| 3f | Alerting Indicators |
| **4** | Indications and Warnings | 4a | Events and Alerts |
| 4b | Warnings |
| 4c | Impact Assessments |
| 4d | Potential Indicators |
| **5** | Vulnerability Knowledge | 5a | Vulnerabilities |
| 5b | Exploits |
| 5c | Potential Victim Information |
| **6** | Mitigation Strategies | 6a | Coordinated Action Plans |
| 6b | Courses of Action |
| 6c | Understanding of Achievable Mitigation Effects |
| **7** | Mitigation Actions and Responses | 7a | Tasking and Status |
| 7b | CNO Capability Awareness |
| 7c | Effectiveness Reporting |
| 7d | After-Action / Lessons Learned Information |

Each ISA Participant is responsible for performing at least one of the ISA Functions, and thus inherits the responsibility to create, exchange and/or ingest some of the identified EFEs; however, each Participant's mission-specific operations will guide how many, and how much of each of these functions they are able to perform. The interdependencies of these functions and exchanges are captured in the figure below, where the functions are represented by the ovals, and the bracketed numbers correspond to the EFEs described in the above table. These combined set of ISA components form the basis for the requirements.



Enduring Functional Exchanges (EFEs) are categories of information that are exchanged on an ongoing basis to promote and enhance IOA, planning, and multiple levels of SSA. These categories contain a number of more specific information flows that would feed or be produced by center processes. The seven EFEs are defined below:

### Configuration/ Anomaly Reporting

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Configuration/ Anomaly Reporting | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Configuration/Anomaly Reporting includes information that describes the configuration and status of a network. This configuration information is critical in determining the risk exposure to vulnerability or a specific exploitation strategy. The status information includes the reporting of network behavior that is unusual but has not been characterized as malicious.   * + - Risk Posture: Configuration-specific status of the relative exposure of a network to a specified vulnerability     - Anomalies: Events or alerts indicating unexpected network behavior or traffic     - Infrastructures: Detailed configuration or other network information that may be requested because of an active or projected exploit to determine risk to or posture of an enterprise; information necessary to determine applicability of vulnerability information | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Knowledge of Threat Actors

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Knowledge of Threat Actors | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Knowledge of Threat Actors consists of the information and analysis products that are available to, and developed by, ISA Participants.   * + - Threat Actor Infrastructure: Information specific to actor techniques, intent, means, and history     - Threat Actor Personas: Information that provides a correlation between actor intent and the capabilities of individual actors     - Threat Actor Attribution: Association of a specific activity to an entity. This can be based on specific exploits used and associated tradecraft     - Trend Analysis: Analysis and characterization of threats across domains, across specific spaces, or globally     - Victim Information: Information regarding potential or exploited victims of specific threat actors     - Threat Actor Indicators: Indicators specific to a threat actor (Signatures are descriptors of threat activity that are characterized so they can be used as mechanisms to monitor, detect, or intercept future instances of the same events.) | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Incident Awareness

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Incident Awareness | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Incident Awareness consists of exchanges that encompass information about "What Am I Seeing"?   * + - Incident Information: Description and characterization of emerging and ongoing events and incidents; these specifics would be used to create alerts or warnings issued to peer organizations     - CNO Awareness: Awareness of current and planned CNO operations that would prevent the activity being characterized as malicious     - Incident Data: Data related to an incident that is shared for the purpose of analysis, mitigation or signature development (i.e., actual malware or Packet Capture File format files)     - Infrastructure Impact/Effects: Impacts and effects of the incident on the infrastructure     - Victim Information: Compromised entities associated with a specified incident     - Alerting Indicators: Descriptors of threat activity that can be characterized so they can be used as mechanisms to monitor or intercept future instances of the same events. | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Indications & Warnings

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Indications & Warnings | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Indications and Warnings are the information items that can provide time critical notification and alerting criteria.   * + - Events and Alerts: NRT notifications that will spur actions or assessment at other partners. Tipping and cueing are a specialized form of alerting that is exchanged through dedicated information channels.     - Warnings: Net speed-level notifications that indicate a specific, emergent risk associated with a confirmed threat. Warnings would include flash-level notifications of detected events, threats, or findings of national significance, CRITICs.     - Impact Assessments: Net speed-level notifications that indicate the relative risk to operations as determined by a domain; may range from a general indicator of change in Cyber Condition (CYBERCON) to a more detailed indicator of mission achievability     - Potential Indicators: Descriptors of threat activity that can be characterized so they can be used as mechanisms to detect future instances of the same events Threat Actor Indicators: Indicators specific to a threat actor (Signatures are descriptors of threat activity that are characterized so they can be used as mechanisms to monitor, detect, or intercept future instances of the same events.) | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Vulnerability Knowledge

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Vulnerability Knowledge | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Vulnerability Knowledge consists of the discovered vulnerabilities in software, hardware, and infrastructure components. This allows for the assessment of the exposure level of specific networks or organizations relative to a specific vulnerability.   * + - Vulnerabilities: Technical design or implementation flaws in IT products or systems that permit exploitation or attack by an unauthorized party     - Exploits: Known intrusion and exploitation techniques or patterns (may or may not be directly correlated to vulnerabilities) that can be mitigated     - Potential Victim Information: Information about entities that are of high risk to a vulnerability or exploit | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Mitigation Strategies

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Mitigation Strategies | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Mitigation Strategies consist of the sets of actions that can be executed to reduce the impact or possibility of an intrusion or to a vulnerability exposure.   * + - Coordinated Action Plans: Integrated action plans developed across multiple domains, including equities, dependencies, and sequencing     - Courses of Action: Preplanned and approved integrated action plans that can be configured on defensive systems for machine-speed execution     - Understanding of Achievable Mitigation Effects: Operational characterization of available capabilities | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Mitigation Actions and Responses

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Knowledge of Threat Actors | |
| Organization | ESSA | |
| Security Classification | Unclassified | |
| Use Case Description | Mitigation Actions and Responses are specific steps that are used to reduce or prevent the impact of an intrusion or vulnerability.   * Tasking and Status: Tasking and confirmation messaging intended to communicate direction or status regarding action plan execution. * Computer Network Operations (CNO) Capability Awareness: Knowledge of possible CNO activities that can be employed to mitigate a threat. * Effectiveness Reporting: Communication of effectiveness of mitigation activities at the national, mission, or operational level (versus IT or CND configuration level, part of the IT Configuration EFE). * After-Action/Lessons Lessons Learned Information: Information regarding closure of action or effectiveness efforts. | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario |  | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

## Victim Notifications

Victim Notification is a critical component of the threat modeling initiative. In the Justice and Public Safety community, significant attention has been devoted to ensure that crime victims and survivors have opportunities to be safely and actively engaged participants in their cases and in the overall justice process. A victim’s right to notification and information about his or her case has long been considered a “threshold right” from which all other victims’ rights flow, and is articulated in state law, Victims’ Bill of Rights, 33 state constitutions, and federal law. When victims are informed about the status of a criminal case and the custody status of an alleged or convicted offender, it empowers them to more safely participate in justice processes and make decisions related to other critical needs, including protection, support services, restitution, and victim compensation. Informed victims are also encouraged to voice their recommendations in plea agreements, sentencing, and parole decisions through victim impact statements. - See more at: <http://savinonline.org>

From a broader threat modeling perspective, victims of cyber threats may be categorized as:

* Victim information compromised as part of a cyber-intrusion
* Victim is directly involved in a cyber-enabled crime

### Victim information compromised as part of a cyber-intrusion

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Victim information compromised as part of a cyber-intrusion | |
| Organization |  | |
| Security Classification | Unclassified/Classified (depending on the type of exposure) | |
| Use Case Description | This use case describes the scenario where the victim is one of a number of victims where their personal information has been compromised but no tangible damage has been inflicted (yet). This scenario would involve an entity that holds the information compromised, and a number (1 or more) of individuals or entities that may be impacted by this compromise. | |
| Key Stakeholders | | |
| Producers | Compromised Entity | |
| Consumers | Victim advocates, victim counselors, victims (individuals and/or entities), monitoring service providers, etc. | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario | * Privacy related information compromised: This would include credit cards, social security numbers, health records, etc. * Protected artifacts, secrets, industrial designs, etc. | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Type of data elements include information about:   * The victim * The compromised entity * Incident details * Mitigation options * Instructions on next steps | | |

### Victim is directly involved in a cyber-enabled crime

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Use Case Description | | | | | |
| Title | | Victim is directly involved in cyber related crime | | | |
| Organization | | Law Enforcement | | | |
| Security Classification | | Unclassified/Classified (depending on the type of exposure) | | | |
| Use Case Description | | This use case describes the scenario where the victim is an entity or an organization where a specific criminal activity has been committed leading to emotional physical or financial damage. | | | |
| Key Stakeholders | | | | | |
| Producers | | Victim advocates, victim counselors, victims (individuals and/or entities), monitoring service providers, etc. | | | |
| Consumers | | Law enforcement, compliance entities, etc. | | | |
| Data Elements | | | | | |
| Action | | Data Elements | | Definitions | |
| Notifications | Notifications | | | |
| ReportingAgency | |  | |
| Recipient | |  | |
| NotificationType | |  | |
| NotificationDate | |  | |
| Notification Subject | |  | |
| Notification Case Reference | |  | |
| NotificationMessage | |  | |
| NotificationActionByDate | |  | |

## Justice and Public Safety

Justice and Public safety is a very broad topic area, and as such should have a large number of use cases that would be relevant to this effort. Here is an initial sampling to highlight broader aspects of cyber. These use cases will be elaborated to include more patterns, reference scenarios, and other categories as they are identified.

From a broader threat modeling perspective, Justice and Public Safety use cases may be categorized as:

* Cyber Intrusion sharing
* Cyber Enabled crimes / Investigatory Referrals

### Cyber Intrusion Sharing

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Cyber Intrusion Sharing | |
| Organization |  | |
| Security Classification | Unclassified/Classified (depending on the type of exposure) | |
| Use Case Description | This use case focuses on sharing information about intrusion, and associated indicators, reports and impact for justice and public safety systems impacted. | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Use Case Details | | |
| Assumptions |  | |
| Exchange Scenario | * DDos attacks * Malware sharing * Systems down * Websites defaced/repurposed * Criminal data altered | |
| Business Rules |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Cyber Enabled crimes/ Investigatory Referrals

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Cyber Enabled crimes / Investigatory Referrals | |
| Organization | Law Enforcement | |
| Security Classification | Unclassified/Classified (depending on the type of exposure) | |
| Use Case Description | This use case describes the scenario where a specific criminal activity has been committed leading to emotional physical or financial damage. A cyber intrusion may also be treated as a criminal activity if investigated. Other types of crimes may include credit card/ identity theft related frauds, etc. The jurisdiction for the investigations may be determined based on thresholds established for referring cases to FBI where they are beyond a certain threshold, and assigning them to local law enforcement below a certain threshold.  <http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3268&issue_id=22014> | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |

### Fusion Center Cross-Domain Sharing

|  |  |  |
| --- | --- | --- |
| Use Case Description | | |
| Title | Fusion Center Cross-Domain Sharing | |
| Organization | Fusion Center | |
| Security Classification | Unclassified/Classified (depending on the type of exposure) | |
| Use Case Description | This use case describes scenarios where a fusion center supports multiple communities by bridging gaps in structure, format, protocol, and vocabularies to communicate intelligence products that may alert the community to a cross-domain incident while it is happening, or provide a more detailed product that advises the community about the issues, provides indicators that the community of practitioners may leverage to track the anomaly, or provide more detailed recommendations on mitigation strategies, or actions that the community could take to help address the issue | |
| Key Stakeholders | | |
| Producers |  | |
| Consumers |  | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Specific data elements are not available, but here are the ‘types’ of information that may be exchanged to meet the requirements for this use case (depending on the level of detail available at the time of publication of the intelligence product)   * Details about the event including where and when observed, behavior indicators, etc. * Specific details about the malware, behavior if available * Mitigation strategy * Mitigation steps * Acknowledgement of receipt and confirmation of execution of steps | | |

Appendix A—Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Editor** | **Change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |